



クイック リファレンス ガイド

Microsoft Windows XPeベースThin Client t5000シリーズ用

製品番号 : 253378-296

2005年1月

このガイドは、Microsoft Corporationから提供されるMicrosoft Windows XPeに関する標準のドキュメントの補足資料です。このターミナルでの相違点、機能の向上、および追加機能について説明します。

© 2004, 2005 Hewlett-Packard Development Company, L.P.

本書の内容は、将来予告なしに変更されることがあります。

Microsoft、MS-DOS、Windows、およびWindows NTは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

その他、本書に掲載されている会社名、製品名はそれぞれ各社の商標または登録商標です。

HP 製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。**本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。**本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対しては、責任を負いかねますのでご了承ください。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。

以下の記号は、本文中で安全上重要な注意事項を示します。



警告：その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがあるという警告事項を表します。



注意：その指示に従わないと、装置の損傷やデータの損失を引き起こす恐れがあるという注意事項を表します。

クイック リファレンス ガイド

Microsoft Windows XPベースThin Client

t5000シリーズ用

改訂第2版 2005年1月

初版 2004年4月

製品番号：253378-296

日本ヒューレット・パッカード株式会社

はじめに	1
イメージの更新	1
サーバ環境の要件	1
セッション サーバ	1
サポート サーバ	3
Windows XPeの拡張機能	4
ログオン	4
プリインストールされているユーティリティ	6
XPeのデスクトップ	8
[プログラム]メニューの拡張項目	11
[コントロール パネル]の拡張選択項目	12
周辺機器	14
プリンタ	15
オーディオ	16
Microsoft Windows XPe Service Pack 2 (SP2)	17
ネットワークの保護	17
Microsoft Internet Explorer	26
Windows Messenger	26
Windows Media Player 9	26
ユーティリティと設定	27
エンハンスド ライト フィルタ マネージャ	27
ローカル ドライブ	32
ネットワーク ドライブの割り当て	33
ユーザ ログ アカウント	34
リモート管理とファームウェアのアップグレード	36
Altiris Deployment Solution ソフトウェア	36
HP Compaq Thin Client イメージング ツール	37

はじめに

HP Compaq t57x0 Thin Clientモデルは、Microsoft® Windows® XP Embedded (XPe) オペレーティング システムを使用しています。Thin Clientを使用することによって、Citrix Independent Computing Architecture (ICA) と Microsoft Remote Desktop Protocol (RDP) のセッション サービスをホスティングするマシン上のアプリケーション、ファイル、およびネットワーク リソースにアクセスできます。キーボード、マウス、オーディオ/ビデオ、およびディスプレイのデータだけが、ネットワークを通じてThin Clientとセッション サーバ間で伝送されます。

イメージの更新

HPでは、HP Compaq t57x0 Thin Clientのイメージを定期的に更新しています。HPのサポート サイトで、お使いのイメージ バージョン用の情報を提供する重要なドキュメントを確認してください。サポート ドキュメントは次のWeb サイトからアクセスできます。

<http://www.hp.com/support>

このガイドでは、Microsoft Windows XPeについて説明しています。Microsoft Windows XPe Service Pack 2のイメージにより提供される新機能について詳しくは、[17ページの「Microsoft Windows XPe Service Pack 2 \(SP2\)」](#)を参照してください。

サーバ環境の要件

Thin Clientでは、ネットワークを通じてさまざまなサービスを使用します。使用するサービスには、DHCPやDNSなどの標準のネットワーク サービスに加えて、セッション サービスや製品サポート サービスも含まれます。以下のセッション サービスとサポート サービスが必要となります。

セッション サーバ

お使いのThin Clientが接続されているネットワークで、以下のセッション サービスを使用できる必要があります。

Citrix ICA

以下のサービスのどちらかを使用すると、ネットワークでCitrix Independent Computing Architecture (ICA) を利用できるようになります。

- Microsoft Windows 2000 Server (ターミナル サービスおよび以下のどちらかがインストールされていること)
 - ❑ Citrix MetaFrame 1.8 (単独、またはService Packs 2か3 FR1を追加)
 - ❑ Citrix MetaFrame XP
- Microsoft Windows NT[®] 4.0 Terminal Server Edition (Citrix MetaFrame 1.8がインストールされていること)

Microsoft RDP

Microsoft Remote Desktop Protocol (RDP) サービスは、Thin Client上のターミナル サービス クライアント アプリケーションによってアクセスされます。以下のサービスのどれかを使用すると、ネットワークでRDPを利用できるようになります。

- Microsoft Windows 2000 Server (ターミナル サービスがインストールされていること)
- Microsoft Windows NT 4.0 Terminal Server Edition
- Microsoft Windows XP Professional
- Microsoft Windows Server 2003



Windows 2000のサーバがICAとRDPの両方のセッション サービスに使用されている場合は、ターミナル サービス クライアント アクセス ライセンス (TSCAL) サーバもネットワーク上に存在する必要があります。クライアント アクセス ライセンスによって、クライアントはWindows 2000 Serverが提供するターミナル サービス、ファイル サービス、プリント サービス、およびその他のネットワーク サービスの使用が許可されます。サーバは90日間有効の一時的なライセンスをデバイス単位で提供します。その期間を超えた場合は、TSCALを購入してTSCALサーバにインストールする必要があります。一時的または永続的なライセンスがなければ、接続することはできません。

Microsoftターミナル サービスの詳細については、MicrosoftのWebサイト (<http://www.microsoft.com/japan/windows2000/technologies/terminal/default.asp>) を参照してください。

ターミナル エミュレーション サポート

Thin Clientのモデルによっては、以前のプラットフォームでの処理をサポートするために、サードパーティ製のターミナルエミュレーション ソフトウェアがインストールされています。ターミナルエミュレーション ソフトウェアは、Telnetプロトコルを使用してプラットフォームと通信します。

サポート サーバ

以下のサポート サーバをThin Clientネットワークで使用することができます。

Altiris Deployment Solution

Altiris Deployment Solutionは、Thin Clientのリモート管理を行うための使いやすい統合ツールです。初期の展開、継続的な管理、ソフトウェアの展開など、Thin Clientのライフサイクル全体を管理できます。

Altiris Deployment Solutionは、Windows NT 4.0またはWindows 2000 Serverにインストールするか、指定されたネットワーク サービスを提供するドメインに管理者としてログオンでき、Thin Clientのソフトウェア リポジトリにアクセスできるワークステーションにインストールする必要があります。Altiris Deployment Solutionsソフトウェアは、工場出荷時にインストールされているPreboot Execution Environment (PXE) クライアント ユーティリティを通じてThin Clientにアクセスします。PXEのアップグレード サービスはAltiris Deployment Solutionに組み込まれています。

Altiris Deployment Solutionについて詳しくは、AltirisのWebサイト (www.altiris.com/documentation、英語サイト) にある『Altiris Deployment Solution User Guide』を参照してください。

Windows XPeの拡張機能

Microsoft Windows XPeベースのThin Clientのオペレーティング システムには、標準のMicrosoft Windows XPオペレーティング システムにはない拡張機能が追加されています。Microsoft Terminal Server Client（リモート デスクトップ接続マネージャ）とCitrix Program Neighborhood、および特注のターミナルエミュレーション アプリケーション（インストールされている場合）を除いて、Windows XPeの拡張機能を制御できるのはAdministratorとしてログオンしたアカウントだけです。



注意：Thin Clientでは、セキュリティ保護のため、またフラッシュへの過度の書き込み処理を防ぐために、書き込みフィルタが採用されています。Thin Clientの設定を変更した場合、変更内容はThin Clientの再起動時に失われます。これを防ぐには、現在のブートセッション中に書き込みフィルタ キャッシュを無効にするか、-commit コマンドを実行します。キャッシュを無効にする方法については、[17 ページの「Microsoft Windows XPe Service Pack 2 \(SP2\)」](#)の書き込みフィルタに関する説明を参照してください。変更内容を永続的に保持しない場合は、常に書き込みフィルタを有効にしておいてください。

ログオン

Thin Clientへのログオンには、自動ログオンまたは手動ログオンを使用できます。

自動ログオン

XPeベースのThin Clientのデフォルトのログオン設定は自動ログオンです。管理者は[コントロール パネル]→[パフォーマンスとメンテナンス]→[管理ツール]の順に選択して表示される[HPログオン マネージャ]を使用して、自動ログオンの有効/無効の切り替えと、自動ログオンのユーザ名、パスワード、およびドメインの変更を行うことができます。自動ログオンのプロパティを変更できるのは、Administratorとしてログオンしたアカウントだけです。



変更を保存するには、現在のブートセッション中に書き込みフィルタ キャッシュを無効にするか、**-commit**コマンドを実行してください。書き込みフィルタの詳細と書き込みフィルタを無効にする方法については、このガイドの[27 ページの「エンハンスドライト フィルタ マネージャ」](#)を参照してください。変更内容を永続的に保持しない場合は、書き込みフィルタを有効にしておいてください。

自動ログオンが有効な場合、**[Windowsへログオン]**ダイアログ ボックスは表示されません。自動ログオンが有効な場合に別のユーザとしてログオンするには、**[Shift]**キーを押しながら**[スタート]→[ログオフ...]**の順にクリックします。**[Windowsへログオン]**ダイアログ ボックスが表示され、ログオン情報を手動で入力できます。

手動ログオン

自動ログオンが無効な場合は、Thin Clientの起動時に**[Windowsへログオン]**ダイアログ ボックスが表示されます。

[ユーザー名]と**[パスワード]**の各テキスト ボックスにログオン情報を入力します。以下の点に注意してください。

- ユーザのログオンアカウントの場合、工場出荷時に設定されているデフォルトのユーザ名とパスワードはどちらも「**User**」です（両方のテキストボックスに入力します）。
- 管理者のログオンアカウントの場合、工場出荷時に設定されているデフォルトのユーザ名とパスワードはどちらも「**Administrator**」です（両方のテキストボックスに入力します）。



セキュリティ保護のため、パスワードをデフォルト値から変更することをおすすめします。管理者は、**[Ctrl] + [Alt] + [Del]** キーを押して**[Windowsのセキュリティ]**ダイアログ ボックスを表示し、**[パスワードの変更]**を選択して、パスワードを変更できます。ユーザとしてログオンしている場合は、パスワードを変更できません。



パスワードの大文字と小文字は区別されますが、ユーザ名では区別されません。



管理者は、コントロールパネルの[管理ツール]オプションにある[ユーザ アカウント]ユーティリティを使用して、ユーザ アカウントを追加できます。ただし、ローカルメモリの容量には制限があるため、追加するユーザの数を最小限にとどめる必要があります。手順については、このガイドの[34ページの「ユーザ ログ アカウント」](#)を参照してください。

管理者ログオンへのアクセス

管理者ログオンにアクセスするには、Thin Clientのユーザ モードの状態に関係なく、次の操作を行います。

[Shift]キーを押したまま、マウスを使用して**[スタート]**メニューからユーザをログオフします。

Administratorとしてログオンするための画面が表示されます。



管理者アカウントの場合、デフォルトのユーザ名およびパスワードは「Administrator」です。ユーザ アカウントの場合、デフォルトのユーザ名およびパスワードは「User」です。

HP Managerアプリケーションを使用して、デフォルトのログイン ユーザを永続的に変更できます。このアプリケーションは[コントロール パネル]にあり、管理者だけがアクセスおよびユーザの変更を行えます。

プリインストールされているユーティリティ

Thin Clientには、いくつかのユーティリティがプリインストールされています。以下のセクションでは、これらのユーティリティについて説明します。

Altiris Client Agent

Altiris Client Agentは、Thin Client上に常駐します。Altirisサーバは、このエージェントを使用して、ネットワークに追加されている有効なクライアントを検出します。このエージェントは、指定された作業を実行し、各Thin Clientの状態をAltirisサーバに報告します。

Citrix Program Neighborhood

Citrix Program Neighborhoodは、MetaFrame 1.8とともに導入されるICAの機能で、ユーザはこの機能を使用してMetaFrameサーバとWinFrameサーバ、および公開されているアプリケーションに接続できます。Citrix Program Neighborhoodによって、アプリケーションへのアクセスを完全に管理し、より高いレベルでデスクトップをシームレスに統合できます。

エンハンスド ライト フィルタ マネージャ

エンハンスド ライト フィルタ マネージャ ユーティリティは、システムと同時に自動的に起動されます。書き込みフィルタによってセキュリティが確保され、過度の書き込み処理からフラッシュ メモリを保護することができます。書き込みフィルタについては、このガイドの[27ページの「エンハンスド ライト フィルタ マネージャ」](#)を参照してください。



Thin Clientの設定を変更した場合、変更内容はThin Clientの再起動時に失われます。これを防ぐには、現在のブートセッション中に書き込みフィルタ キャッシュを無効にするか、`-commit`コマンドを実行します。書き込みフィルタを無効にする方法については、このガイドの[27ページの「エンハンスド ライト フィルタ マネージャ」](#)を参照してください。変更内容を永続的に保持しない場合は、書き込みフィルタを有効にしておいてください。

Macromedia Flash Player

Macromedia Flash Playerは、複数のプラットフォーム間でWebの豊富な機能を共有できるエージェントです。Macromedia Flash Playerによって、世界中のWebユーザが、Macromedia Flashで作成されたコンテンツの表示や対話を行うことができます。

リモート デスクトップ接続

Microsoft リモート デスクトップ接続を使用すると、管理者はリモートに設置されたWindows XPベースのThin Clientにアクセスできます。管理者は、この接続を利用して、ローカルのThin Clientとアプリケーションを制御できます。

XPeのデスクトップ

ここでは、XPeのユーザと管理者のデスクトップ機能の概要を説明します。

ユーザのデスクトップ

ユーザとしてログオンした場合に表示されるデスクトップは、標準のWindows XPデスクトップと同じです。ただし、表示されるアイコンは、[Citrix Program Neighborhood]、[Remote Desktop Connection]、および[Internet Explorer]だけです。これらは、[スタート]メニューから選択することもできます。ターミナルエミュレータアプリケーションがインストールされている場合は、[スタート]→[プログラム]メニューの順に選択して開くことができます。



リモートのICA NFuseで公開されているアプリケーションへのリンクも、[スタート]メニューやデスクトップのアイコンとして表示されます。詳しくは、Citrix NFuse 1.6のドキュメントを参照してください。

標準のWindows XPeデスクトップと[スタート]メニューの項目については、以下のWebサイトで該当するMicrosoftのドキュメントを参照してください。

www.microsoft.com/japan/windows/embedded/xp/default.asp

Citrix Program Neighborhoodとリモート デスクトップ接続に関するドキュメントのインターネット上の入手先については、このガイドの11ページの「**[プログラム]メニューの拡張項目**」を参照してください。



[スタート]→[コントロール パネル]の順に選択して表示される[コントロール パネル]からは、Windows XPeのユーザ設定を作成するための一部のリソースにしかアクセスできません。システム リソースの拡張セットにアクセスするには、管理者としてログオンする必要があります。



デスクトップの背景にポインタを置いて右クリックしても、ポップアップメニューは表示されません。



標準のコピーと貼り付けの操作によって、リモートセッションとローカルコンピュータの間でテキストのコピーと貼り付けを行うことができます。

管理者のデスクトップ

管理者としてログオンしている場合に表示されるデスクトップは、標準のWindows XPデスクトップです。管理者のデスクトップにデフォルトで表示されるアイコンは、[Citrix Program Neighborhood]、[Remote Desktop Connection]、および[Internet Explorer]です。3つのアプリケーションは、[スタート]メニューから選択することもできます。ターミナルエミュレータアプリケーションがインストールされている場合は、[スタート]→[プログラム]メニューの順に選択して開くことができます。管理者だけが使用できる拡張リソースには、[スタート]メニューからアクセスできます。

標準のWindows XPeデスクトップと[スタート]メニューの項目については、前のセクションに示したMicrosoftのWebサイトを参照してください。



管理者デスクトップの背景にポインタを置いて右クリックすると、ポップアップメニューが表示されます。

Thin Clientのログオフ、再起動、およびシャットダウン

Thin Clientのログオフ、再起動、シャットダウンを行うには、[スタート]→[シャットダウン]の順にクリックします。[シャットダウン]ダイアログボックスで、該当する操作を選択して[OK]をクリックします。



[Windowsのセキュリティ]ダイアログボックスからログオフまたはシャットダウンすることも可能です。[Ctrl]+[Alt]+[Del]キーを押すと、ダイアログが開きます。



自動ログオンが有効な場合、シャットダウンせずにログオフするとすぐにデフォルトのユーザがThin Clientにログオンします。別のユーザとしてログオンする方法については、このガイドの4ページの「ログオン」を参照してください。

Thin Clientのログオフ、再起動、およびシャットダウンを行うと、以下のユーティリティが影響を受けます。

エンハンスド ライト フィルタ

エンハンスド ライト フィルタについては、このガイドの[27ページの「エンハンスド ライト フィルタ マネージャ」](#)を参照してください。システム設定を変更してその内容を保持するには、現在のブート セッション中に書き込みフィルタ キャッシュを無効にするか、**-commit** コマンドを実行する必要があります。それ以外の場合、変更した設定はThin Clientのシャットダウン時または再起動時に失われます。変更内容を永続的に保持しない場合は、常に書き込みフィルタを有効にしておいてください。

同一ユーザか別ユーザかに関わらず、ログオフ後に再度ログオンする場合、書き込みフィルタ キャッシュの内容は失われません。つまり、新しくログオンした後に書き込みフィルタ キャッシュを無効にしても、変更は保持されます。

書き込みフィルタを無効にする権限は、ユーザのログオン アカウントには与えられていません。これはローカルまたはリモートの管理者が使用できる機能です。

電源の管理

モニタの節電機能によってモニタへのビデオ信号が切断されると、指定されたアイドル時間の経過後、モニタは省電力モードに入ります。省電力モードの値を設定するには、デスクトップの背景で右クリックし、**[プロパティ]**→**[スクリーン セーブ]**→**[電源]**の順に選択します。

システム時刻

電源を切った後でも、電源ケーブルが接続されていれば、時刻設定が失われることはありません。ただし、電源ケーブルが接続されていない場合、時刻設定は失われます。ローカル時刻ユーティリティを使用すると、指定した時刻に、自動的にまたは手動でThin Clientの時計を時刻サーバに同期させることができます。



アプリケーションによってはローカルのThin Clientの時刻を利用する可能性があるため、正しい時刻設定を維持する必要があります。[日付と時刻のプロパティ]ダイアログを表示するには、タスク バーの時刻表示部分をダブルクリックするか、[コントロール パネル]の[日付、時刻、地域と言語のオプション]で[日付と時刻]をダブルクリックします。

[プログラム]メニューの拡張項目

[スタート]→[プログラム]の順にクリックすると、[プログラム]メニューが表示されます。[プログラム]メニューに表示される追加項目は以下のとおりです。

Citrix Program Neighborhood

この項目を選択すると、Citrix Program Neighborhoodのウィンドウが表示されます。このウィンドウはデスクトップのアイコンから表示することもでき、ICAサーバ上で実行中のリモート アプリケーションへの接続を確立するために使用します。

ICAクライアント アプリケーションに関するドキュメントは、以下のCitrix CorporationのWebサイト（英語サイト）で入手できます。

www.citrix.com/support

（「Product Documentation」のページで検索してください）

リモート デスクトップ接続

この項目を選択すると、[リモート デスクトップ接続]ダイアログ ボックスが表示されます。このダイアログ ボックスは、デスクトップのアイコンから表示することもでき、RDPを使用するリモート アプリケーションへの接続を確立するために使用します。[リモート デスクトップ接続]ダイアログ ボックスの詳細と使用方法のドキュメントについては、MicrosoftのWebサイトを参照してください。

TeemNT

ターミナルには、TeemNTターミナルエミュレーション アプリケーションがインストールされています。詳しくは、別途提供されるターミナル エミュレーションのドキュメントを参照してください。デフォルトでは、デスクトップ アイコンはインストールされません。

Internet Explorer

Thin Clientには、Microsoft Internet Explorerのバージョン6.0がローカルでインストールされています。

工場出荷時のブラウザのインターネット オプション設定では、フラッシュ メモリへの書き込みが制限されています。容量に制限のあるフラッシュ メモリを使い切らないための設定なので、変更しないでください。より多くのブラウザ リソースが必要な場合は、ICAまたはRDPを通じて別のブラウザにアクセスできます。ローカルのブラウザは、**[スタート]**メニューまたはデスクトップのアイコンから表示することができます。

[コントロール パネル]の拡張選択項目

[コントロール パネル]ウィンドウは、タスク バーの**[スタート]**をクリックし、**[スタート]**→**[コントロール パネル]**の順に選択すると表示されます。コントロール パネルで利用できる拡張項目の一部を、以下に説明します。

HP RAMディスク

RAMディスクは、データの一時記憶領域として用意されている揮発性メモリの領域です。マイ コンピュータのウィンドウでは、Z:ドライブとして表示されます。

RAMディスクには、以下の項目が格納されます。

- ブラウザのWebページキャッシュ
- ブラウザの履歴
- ブラウザのcookie
- ブラウザのキャッシュ
- インターネット一時ファイル
- 印刷スプール
- ユーザおよびシステムの一時ファイル

管理者の判断により、RAMディスクを上記以外のデータ（移動プロファイルなど）の一時記憶領域として使用することもできます（このガイドの[32ページの「ローカル ドライブ」](#)を参照してください）。

[HP RAMディスク マネージャ]ダイアログ ボックスを使用して、RAMディスクのサイズを設定します。RAMディスクのサイズを変更すると、変更内容を有効にするために再起動を促すメッセージが表示されます。ただし、変更内容を保持するには、再起動前の現在のブートセッション中に書き込みフィルタ キャッシュを無効にするか、-commitコマンドを実行する必要があります。



RAMディスクのデフォルトのサイズは、Thin Clientのモデルおよび取り付けられているメモリ サイズによって異なります。RAMディスクのサイズに設定できる最大値は64 MB、最小値は2 MBです。

地域と言語のオプション

キーボードの言語オプションは、工場出荷時にあらかじめ設定されています。必要に応じて、[コントロール パネル]の[日付、時刻、地域と言語のオプション]で[地域と言語のオプション]からキーボードの言語を変更できます。このプログラムでは、使用するキーボードの種類、およびレイアウトとIMEの設定を選択できます。

管理ツール

[コントロール パネル]の[パフォーマンスとメンテナンス]で[管理ツール]アイコンをクリックすると、管理ツールを選択するウィンドウが表示されます。

サービス

[サービス]を選択すると、[サービス]ウィンドウが開き、Thin Clientにインストールされているサービスの一覧が表示されます。

ユーザ マネージャ

ユーザ マネージャは、管理者がユーザ アカウントの作成、削除、および管理を行うためのユーティリティです。詳しくは、このガイドの[34ページ](#)の「[ユーザ プロファイル](#)」を参照してください。

周辺機器

デバイスに対応するソフトウェアがインストールされていれば、Thin Clientで使用可能なポートによって、USB、シリアル、パラレル、およびPCIの各種デバイスのためのサービスを提供できます。工場出荷時にインストールされるソフトウェアについては、以下のセクションで説明します。その他のサービスのアドオンは、利用可能になり次第、Altiris Deployment Solution ソフトウェアを使用してインストールすることができます（[37ページの「ファームウェアのアップグレード」](#)を参照してください）。

USB/シリアル変換ケーブル

USB/シリアル変換ケーブルでThin Clientに接続しているデバイスに割り当てられるポートを確認するには、以下の手順で操作します。

1. プリンタなどのデバイスを変換ケーブルのシリアル ポートに接続します。このとき、変換ケーブルのUSB コネクタをThin Clientに接続しないでください。
2. [デバイス マネージャ]ウィンドウを開きます（[コントロール パネル]→[パフォーマンスとメンテナンス]→[システム]→[ハードウェア]タブ→[デバイス マネージャ]の順にクリックします）。
3. Thin Clientのモデルによっては、またデバイス ドライバがすでにポートにインストールされているかどうかによっては、ポート（COMとLPT）の一覧が表示されない場合もあります。一覧が表示されている場合は、項目を展開して使用中のポートを表示します。
4. 変換ケーブルのUSBコネクタをThin Clientに接続します。
5. ポート（COMとLPT）の一覧が表示されていなかった場合は、この時点で表示されます。ポート（COMとLPT）の一覧に、新しい接続に対応する新しいCOMポートが表示されます。新しい接続に割り当てられたCOMポート番号を書き留めておきます。
6. メッセージが表示されたら、検出されたポート番号を使用して接続したデバイスのインストール手順を続けます。シリアル タッチ スクリーンなどのデバイスについては、製造元の手順に従ってください。



USB/シリアル変換ケーブルは、同時に2本まで使用可能です。

プリンタ

Thin Clientにはユニバーサル プリント ドライバがインストールされており、ローカル接続プリンタへのテキストのみの印刷をサポートしています。ローカル接続プリンタでテキストのすべての設定および画像の印刷を行うには、製造元が提供するドライバをインストールし、製造元の指示に従ってください。インストールしたことによる設定を保存するには、書き込みフィルタ キャッシュを無効にするか、**-commit**コマンドを実行します。ICAやRDPのアプリケーションからネットワーク プリンタに印刷するには、サーバ上のプリント ドライバを使用します。



注意：フラッシュ メモリの空き領域が3 MB未満になると、Thin Clientの動作が不安定になります。



プリンタを機能させ、ダウンロードするためには、十分なフラッシュ メモリ領域が必要です。場合によっては、ソフトウェア コンポーネントを削除して、プリンタのために空き領域を確保する必要があります。



サーバのプリント ドライバを使用してICAまたはRDPのセッションからローカル接続されたプリンタへ印刷する場合、テキストのすべての設定および画像の設定を印刷できます。これを行うには、プリント ドライバをサーバにインストールし、テキストのみに対応したドライバをThin Clientにインストールする必要があります（次のセクションを参照してください）。

汎用のテキスト専用プリント ドライバを使用したプリンタの追加

テキスト専用プリント ドライバを使用してプリンタを追加するには、以下の手順で操作します。

1. プリンタをパラレル ポートに接続します。
2. [スタート]→[プリンタとFAX]の順に選択します。
3. [プリンタのインストール]をクリックします。プリンタの追加ウィザードが表示されます。
4. ウィザードの最初のパネルで[次へ]をクリックします。
5. [このコンピュータに接続されているローカル プリンタ]ラジオ ボタンをオンにします。

-
6. [プラグ アンド プレイ対応プリンタを自動的に検出してインストールする]チェック ボックスがオフになっていることを確認します。
 7. [次へ]をクリックします。
 8. [次のポートを使用]ラジオ ボタンをオンにします。
 9. ドロップダウン リストから該当するポートを選択し、[次へ]をクリックします。
 10. プリンタの製造元とモデルを選択して、[次へ]をクリックします。
 11. プリンタに割り当てられているデフォルトの名前または別の名前を指定して、[次へ]をクリックします。
 12. [このプリンタを共有しない]ラジオ ボタンをオンにして、[次へ]をクリックします。
 13. テスト ページを印刷するかどうかを選択して、[次へ]をクリックします。
 14. [完了]をクリックします。
 15. インストールが完了し、テスト ページの印刷を選択した場合はページが印刷されます。

製造元が提供するプリント ドライバの使用

製造元が提供するドライバをインストールし、製造元の指示に従って操作します。インストールを保存するには、書き込みフィルタ キャッシュを無効にするか、-commitコマンドを実行します。

オーディオ

オーディオは、アプリケーションからThin Clientのオーディオ コネクタへリダイレクトされる場合があります。オーディオのレベルは外部から（600 Ω の可変抵抗器などによって）制御する必要があり、スピーカを駆動させるにはパワー ブースタが必要です。タスク バーのシステム トレイに表示されているサウンドアイコンを使用して、音量を調整できます。このアイコンをシングルクリックすると、音量調整のマスタ画面が表示されます。また、ダブルクリックすると、音量調整アプリケーションのダイアログ ボックスが表示されます。

Microsoft Windows XPe Service Pack 2 (SP2)

Microsoft Windows XPe Service Pack 2 (SP2) では、パーソナルコンピュータの新しいセキュリティ対策として、オペレーティング システムの基本的な機能の多くが改善されています。

HP Compaq Thin ClientのMicrosoft Windows XPe SP2イメージには、以下の機能に対する改善点が含まれます。

- ネットワークの保護
- Microsoft Internet Explorer
- Windows Messenger
- Windows Media Player

ネットワークの保護

ネットワークの保護はWindows XPe Service Pack 2の最大の改善点であり、既存のソフトウェアに最も大きな影響を与えます。

Sygate Firewall

HPのXPe SP2イメージには、Sygate Firewallが含まれます。HP Sygate Security Agentで提供されるカスタマイズ可能なファイアウォールは、コンピュータへの第三者による侵入およびコンピュータの誤用を、その悪意の有無にかかわらず防止するために役立ちます。このエージェントは、既知のトロイの木馬、ポート スキャン、およびその他の一般的な攻撃を検出して特定します。また、さまざまなネットワーク サービス、アプリケーション、ポート、およびコンポーネントの使用を許可またはブロックすることでそれらに対処できます。

HP Sygate Standalone Agentには、アプリケーションまたはトラフィックの署名によって、着信時または送信時のポートまたはプロトコルを許可またはブロックする機能があります。このエージェントでは、これらのパラメータに基づいたブロックを行うだけでなく、パラメータを論理ステートメントや条件ステートメントに結び付けることができるため、適用できるポリシーの範囲が広がり、柔軟性が向上しています。さらに、このエージェントはカスタマイズされたプロトコルアダプタに対するポリシーの適用およびブロックを行うため、企業はネットワーク対応のカスタマイズされたアプリケーションを使用することや、カスタマイズされたプロトコルアダプタによってTCP/IPスタックを回避するアプリケーションをブロックすることができます。

Sygate Firewallについて詳しくは、以下のWebサイトにあるホワイトペーパー『HP Sygate Security Agent: Frequently Asked Questions』（英語版）を参照してください。

<http://h200006.www2.hp.com/bc/docs/support/SupportManual/c00282639/c00282639.pdf>

Microsoft Windowsファイアウォール

改善されたMicrosoft Windowsファイアウォール（以前のインターネット接続ファイアウォール（ICF））は、HPからアドオンとして提供されています。アドオンをインストールすると、ファイアウォールはデフォルトで有効になります。



Microsoft Windowsファイアウォールはアドオンとしてのみ提供され、イメージには含まれません。Microsoft Windowsファイアウォールをインストールする前に、Sygate Firewallを削除する必要があります。Sygate Firewallを削除するためのアドオンは、以下のWebサイト（英語サイト）で入手できます。

<http://h18004.www1.hp.com/support/files/thinclients/us/download/22239.html>

デフォルトでの有効化

アドオンをインストールすると、Windows ファイアウォールはすべてのネットワーク インタフェースに対してデフォルトで有効になります。また、この機能により、新しいネットワーク接続がシステムに追加されるたびにその接続が保護されます。その結果、アプリケーションがデフォルトでステートフル フィルタリングに対応していない場合は、アプリケーションの互換性が損なわれる可能性があります。

Microsoft Windowsファイアウォールの設定

Windows ファイアウォールでは、最適なセキュリティと使いやすさを提供するため、トラフィックを受信可能にしたいアプリケーションやサービスがある場合は、それらを例外として設定できます。

Windows ファイアウォールを設定するには、[コントロール パネル]からファイアウォールにアクセスします。また、ネットワーク接続のプロパティを表示するウィンドウの[詳細設定]タブからもアクセスできます。

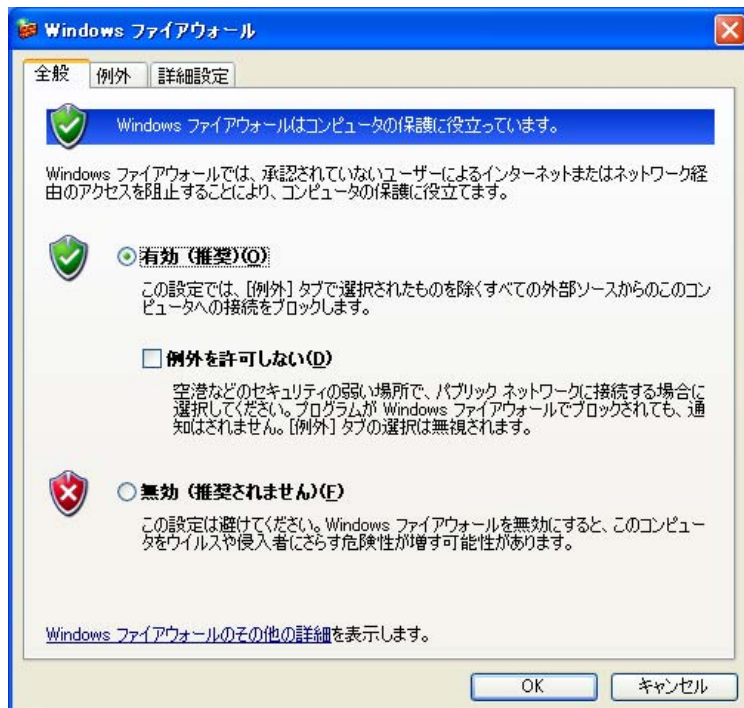
セキュリティ センターはイメージに含まれていません。Windows ファイアウォールのアドオンを適用すると、コントロール パネル アプレット FIREWALL.CPLは管理者のアカウントでのみ使用可能になります。



Windows ファイアウォールのアドオンを起動すると、コントロール パネル アプレットは管理者のアカウントでのみ使用可能になります。

■ [全般]タブ: [全般]タブでは、次の3つの主要なオプションを設定します。

- ☐ 有効 (推奨)
- ☐ 例外を許可しない
- ☐ 無効 (推奨されません)



[例外を許可しない]を選択すると、Windowsファイアウォールにより、コンピュータへの接続要求が、[例外]タブで設定したプログラムやサービスからの要求を含めてすべてブロックされます。また、ファイルとプリンタの共有、およびネットワーク デバイスの検出もブロックされます。

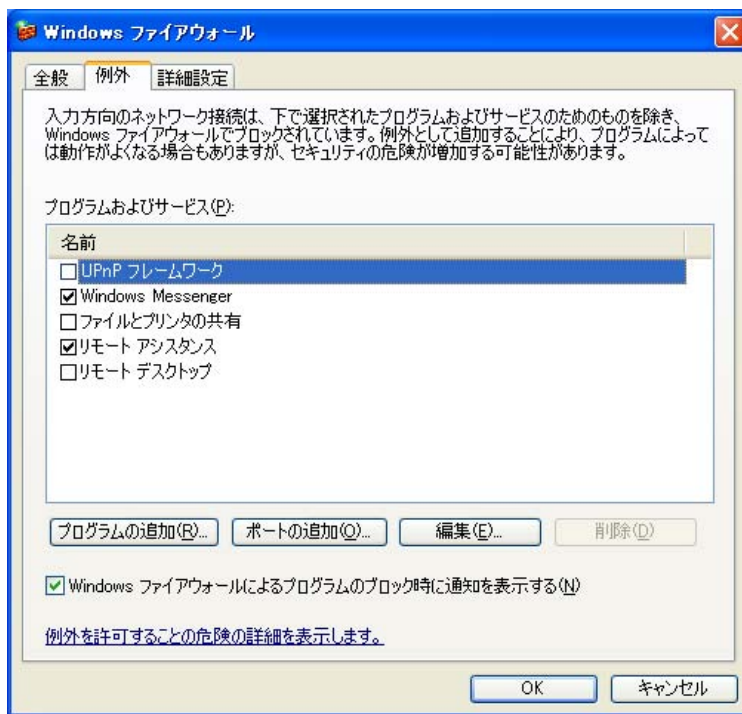
空港やホテルなどの公共のネットワークに接続するときには、Windowsファイアウォールで例外を許可しない設定が役立ちます。この設定によってコンピュータへの接続がすべてブロックされ、コンピュータを保護することができます。

Windowsファイアウォールで例外を許可しない場合でも、Webページの閲覧、電子メールの送受信、およびインスタントメッセージプログラムの使用は可能です。

- **[例外]タブ**：特定の種類の受信トラフィックを許可するプログラムやポートを例外として追加できます。例外の設定では、ポートやプログラムをどのコンピュータに対して開放するかを指定します。

次の3つのアクセス モードを指定できます。

- ☐ 任意のコンピュータ（インターネット上のコンピュータを含む）
- ☐ ユーザのネットワーク（サブネット）のみ
- ☐ カスタムの一覧

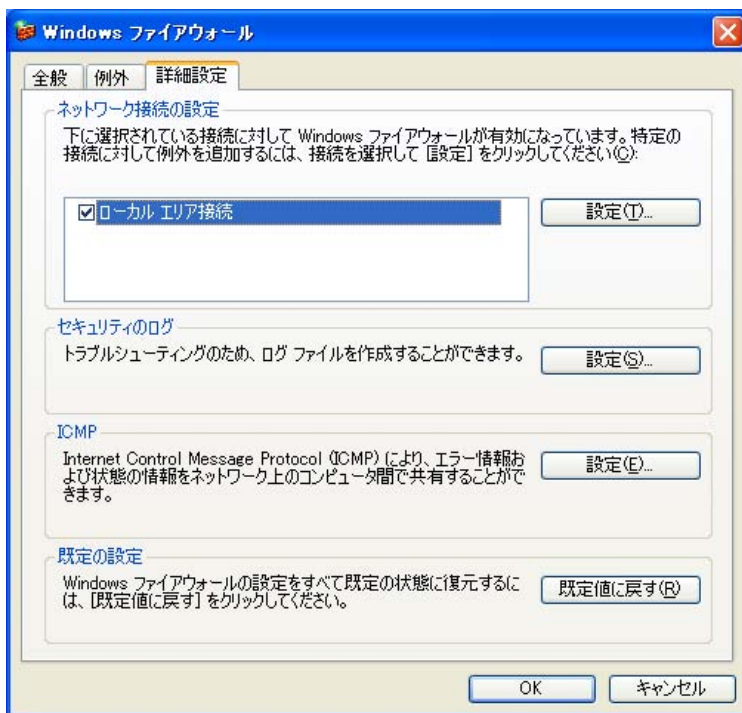


デフォルトでは、[Windowsファイアウォールによるプログラムのブロック時に通知を表示する]チェックボックスにはチェックが入っています。

例外ごとにスコープを設定できます。自宅および小規模なオフィスのネットワークでは、可能な場合はローカル ネットワークだけにスコープを設定することをおすすめします。この設定によって、同じサブネット上のコンピュータはお使いのマシン上のプログラムに接続できますが、リモート ネットワークからのトラフィックは破棄されます。

■ [詳細設定]タブ：以下の機能を設定できます。

- ☐ [ネットワーク接続の設定]：ネットワーク インタフェースごとに適用する、接続に固有の規則を選択します。
- ☐ [セキュリティのログ]：トラブルシューティングの際に使用するログ ファイルを作成します。
- ☐ [ICMP]：グローバルICMP（Internet Control Message Protocol）を使用することで、ネットワーク上のコンピュータがエラー情報および状態の情報を共有できます。
- ☐ [既定の設定]：Windowsファイアウォールをデフォルトの設定に復元します。



設定情報の収集

Windows ファイアウォールの現在のポリシーの設定は、netsh firewall show configurationというコマンドを実行することで参照できます。

アプリケーションのトラブルシューティング

問題解決のための理想的な方法は、ステートフル フィルタリングを行うファイアウォールを通じて動作するようにアプリケーションの設定を変更することです。この方法が常に可能であるとは限らないため、ファイアウォールではポートとアプリケーションの例外を設定するためのインターフェースが提供されます。

障害の状況

デフォルトの設定に関係する障害は、次の2通りの状態で発生します。

- クライアント アプリケーションがサーバからのデータの受信に失敗します。たとえば、FTPクライアント、マルチメディア ストリーミング ソフトウェア、電子メール アプリケーションの新規メール通知などに発生します。
- Windows XPで動作するコンピュータ上で実行中のサーバアプリケーションが、クライアントの要求に応答しません。たとえば、IIS (Internet Information Services) などの Web サーバ、リモート デスクトップ、ファイル共有などに発生します。



ネットワーク アプリケーションで発生する障害は、ファイアウォールに関する問題ではありません。RPCやDCOMのセキュリティを変更することで障害が発生する場合があります。障害の発生時に、アプリケーションがブロックされていることを示すセキュリティの警告が、Windows ファイアウォールで表示されているかどうかを確認することが重要です。



解決方法

前ページで述べた障害のどちらについても、Windows ファイアウォールの設定に例外を追加することで対処できます。例外を追加することで、コンピュータへの特定の着信接続がファイアウォールにより許可されます。



ポートの追加よりも、プログラムの追加を行うことをおすすめします。プログラムの追加はポートの追加よりも簡単で安全です。使用するポートの番号を知らなくても操作でき、ポートはプログラムが着信接続を待機しているときにのみ開放されるためです。プログラムを追加した場合は、指定されたアプリケーションだけがポートを使用できますが、ポートを開放した場合はどのアプリケーションでもポートを使用できるようになります。

プログラムの追加

例外の一覧にプログラムを追加する設定をおすすめします。これは最も簡単な設定であるだけでなく、この設定により、プログラムを実行するたびに変わるポート範囲をファイアウォールで開放できるようになります。

プログラムの例外を追加するには、以下の手順で操作します。

1. Windows ファイアウォールを開き、**[例外]**タブをクリックします。
2. プログラムが一覧に存在する場合は、クリックして設定を有効にします。プログラムが一覧に存在しない場合は、**[プログラムの追加]**をクリックして**[プログラムの追加]**ダイアログ ボックスを表示します。
3. **[参照]**をクリックし、例外として追加するプログラムを選択してから**[OK]**をクリックします。
4. **[スコープの変更]**をクリックし、プログラムに対するスコープを参照または設定してから**[OK]**をクリックします。
5. **[OK]**をクリックして**[プログラムの追加]**ダイアログ ボックスを閉じます。
6. デフォルトでは、プログラムは一覧で有効になっていません。チェック ボックスをクリックしてチェックを入れ、プログラムを有効にします。

ポートの追加

例外の一覧にプログラムを追加してもアプリケーションの問題が解決されない場合は、ポートを手動で追加します。それにはまず、アプリケーションにより使用されるポートを判別する必要があります。最も信頼性の高い判別方法は、アプリケーションの製造販売元に問い合わせることです。

プロセスのためのポート番号が1024よりも小さい場合、ポート番号は変更されない可能性があります。使用されるポート番号が1024よりも大きい場合、アプリケーションは一定範囲内のポートを使用するので、個々のポートを開放しても問題を解決できないことがあります。

ポート番号とプロトコルが判明したら、ポートの例外を追加します。ポートの例外を追加するには、以下の手順で操作します。

1. Windowsファイアウォールを開き、**[例外]**タブをクリックします。
2. **[ポートの追加]**をクリックして**[ポートの追加]**ダイアログ ボックスを表示します。
 - a. ポート番号を入力します。
 - b. **[TCP]**または**[UDP]**のどちらかのプロトコルを選択します。
 - c. **[名前]**フィールドに、ポートの例外を説明する名前を入力します。
3. **[スコープの変更]**をクリックして、ポートの例外に対するスコープを参照または設定し、**[OK]**をクリックします。
4. **[OK]**をクリックして**[ポートの追加]**ダイアログ ボックスを閉じます。
5. チェック ボックスをクリックしてチェックを入れ、ポートを有効にします。

追加情報

Microsoft Windows Service Pack 2およびMicrosoft Windows ファイアウォールについてさらに詳しく調べるには、以下のWebサイトを参照してください。

- Windows XP Service Pack 2 : 開発者向け情報
<http://www.microsoft.com/japan/msdn/windows/windowsexp/securityinxpsp2.asp>
- TechNet Windows XP Professional Webサイト
<http://www.microsoft.com/japan/technet/prodtechnol/winxppro/default.mspx>
- Windows XP Service Pack 2のWindowsファイアウォールを手動で構成する
<http://www.microsoft.com/japan/technet/community/columns/cableguy/cg0204.mspx>
- Microsoft Windows XP Service Pack 2における Windows ファイアウォール用INFファイルの使用
<http://www.microsoft.com/downloads/details.aspx?FamilyID=eb982f8c-2391-429e-9b26-31e88edfcdf9&DisplayLang=ja>

-
- Microsoft® Windows® XP Service Pack 2向けWindowsファイアウォール設定の導入

<http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=ja>

Microsoft Internet Explorer

Service Pack 2では、Microsoft Internet Explorerの安全性が向上しています。すべてのコンテンツの実行を、より細かく制御できるようになりました。Internet Explorerには、表示したくないポップアップ ウィンドウをブロックし、表示したいポップアップ ウィンドウを管理するための機能が組み込まれました。さらにInternet Explorerでは、スクリプトによるウィンドウおよびステータス バーの移動やリサイズが阻止されるため、ウィンドウやステータスバーが非表示になったり、他のウィンドウが隠れたりすることを防止できます。

Windows Messenger

Windows XPe Service Pack 2のWindows Messengerには、安全でないファイルの送信をブロックする機能が追加されています。

一般的に安全でないと考えられるファイルの一覧については、Microsoft Web サイト (<http://support.microsoft.com/kb/291369/ja>) の『Internet Explorer 6の安全でないファイル (Unsafe File) 一覧に関する情報』を参照してください。

Windows Media Player 9

新しいMedia Playerでは、セキュリティ、パフォーマンス、および機能が向上しています。

Windows Media Player の改善点について詳しくは、Windows Media Player の ホーム ページ (<http://www.microsoft.com/japan/windows/windowsmedia/>) を参照してください。

ユーティリティと設定

このセクションでは、Thin Clientのユーティリティと設定について説明します。

エンハンスド ライト フィルタ マネージャ

エンハンスド ライト フィルタ マネージャは、Thin Clientのコンピュータ機能のための安全な環境を提供します。これは、フラッシュ メモリへの望ましくない書き込みから Thin Clientを保護することで実現されます（フラッシュ メモリには、オペレーティング システムやソフトウェア コンポーネントが格納されています）。また、書き込みフィルタによって、フラッシュ メモリへの過度の書き込み処理を防ぐことで、Thin Clientの寿命を延ばすことができます。キャッシュを使用すると、フラッシュ メモリへの実際の書き込みを行わずに、入出力を要求した処理に対して正常終了を返すことによって、フラッシュ メモリに対する読み取り/書き込みのアクセスを行ったように見えます。

キャッシュに格納されて実際にはフラッシュ メモリに書き込まれなかった内容は、Thin Clientがアクティブである限り有効ですが、Thin Clientが再起動またはシャットダウンされると失われます。レジストリ、お気に入り、cookie などへの書き込み結果を保持するには、キャッシュの内容をフラッシュ メモリに転送する必要があります。これは、Altiris Deployment Solutionソフトウェアによって処理するか、エンハンスド ライト フィルタ マネージャを使用して手動で行います。

書き込みフィルタを無効にすると、現在のブートセッションでのその後の書き込みはすべてフラッシュ メモリに書き込まれます。この場合、再起動されるまで、キャッシュは使用されません。書き込みフィルタは、コマンドラインでも有効/無効を切り替えることができます。永続的な変更がすべて正常に行われた後には、書き込みフィルタを常に有効にしておいてください。

管理者は、定期的にキャッシュの状態を確認する必要があります。キャッシュの使用量が80%を超えた場合は、Thin Clientを再起動する必要があります。



注意：書き込みフィルタ キャッシュが80%を超えた場合は、キャッシュを無効にしないでください。



Thin Clientに永続的な変更を加えるときにフラッシュ メモリが破損することを回避するために、システムに永続的な変更を加える前に書き込みフィルタを無効にしておくことを強くおすすめします。すべての変更が行われた後に書き込みフィルタを有効にしておいてください。

次のセクションでは、コマンドラインで書き込みフィルタを操作する方法について説明します。

エンハンスド ライト フィルタ マネージャのコマンド ラインでの制御



注意：ターミナルの管理者は、Microsoft Windows NT のファイル セキュリティを使用して、以下のコマンドの不正使用を防止する必要があります。



注意：-commitコマンドを実行すると、すべての一時的な内容がフラッシュメモリに永続的に書き込まれます。



エンハンスド ライト フィルタ マネージャのコマンドは次回の起動時に実行されるため、コマンドを有効にするにはシステムを再起動する必要があります。

Windows XPeには、エンハンスド ライト フィルタ (EWF) コンソール アプリケーションのコマンドライン ツール、Ewfmggr.exeが含まれています。このツールを使用して、EWFドライバに対するコマンドセットの実行、保護されているボリューム オーバーレイ ごとの状態の表示、およびEWF設定全体の表示を行うことができます。

EWFマネージャ コンソール アプリケーション コンポーネントをお使いの構成に組み込んでイメージ内に構築することにより、Ewfmggr.exeおよび対応するコマンドを使用できるようになります。

コマンドラインでエンハンスド ライト フィルタ マネージャを使用するには、[スタート]→[ファイル名を指定して実行]の順にクリックし、[名前]フィールドに「CMD」と入力して[OK]をクリックします。システムDOSプロンプトが表示されます。

システム プロンプトで、「**ewfmgr c:**」と入力して **[Enter]** キーを押します。
「ewfmgr <ドライブ文字> -[ブート コマンド]」という構文を使用して、コマンド ラインのブート コマンド変数の部分で以下のコマンドを使用します。

-all

保護されているすべてのボリュームに関する情報を表示し、**disable**、**enable**、**commit**などのコマンドが指定されている場合は、それらのコマンドを各ボリュームに対して実行します。

-commit

オーバーレイ内にある現在のレベルのデータすべてを保護されているボリュームにコミットし、現在のオーバーレイ値を1にリセットします。**-commit**を**-disable**コマンドと組み合わせると、コミット後に無効にすることができます。

-disable

特定の保護されているボリューム上にあるオーバーレイを無効にします。

-enable

エンハンスド ライト フィルタを有効にして、保護されたメディアに書き込まれるデータがオーバーレイにキャッシュされるように設定します。EWFが起動されるとすぐに現在のオーバーレイ レベルは1になり、レベル1の新しいオーバーレイが作成されます。

-commitanddisable

commit コマンドと **disable** コマンドの組み合わせです。シャットダウン時にオーバーレイ内のデータをコミットします。また、システムの再起動後にEWFが無効になります。

エンハンスド ライト フィルタのGUI

Windows XP Embeddedイメージには、DOSコマンドライン ツールに加えて、新たにエンハンスド ライト フィルタ (EWF) のGUIが含まれています。EWFのGUIには、[コントロール パネル]または管理者の[管理ツール]オプションからアクセスできます。EWFのGUIにアクセスするには、以下の手順で操作します。

1. 管理者としてログインします。
2. [スタート]→[コントロール パネル]→[コントロール パネルのその他のオプション]または[スタート]→[コントロール パネル]→[パフォーマンスとメンテナンス]→[管理ツール]の順に選択します。
3. [エンハンスド ライト フィルタ]アイコンをクリックします。
4. EWFのGUIを使用して、書き込みフィルタのオプションを選択します。

EWFのGUIには、以下のボタンが含まれます。

EWF有効

このボタンで、DOSプロンプトのewfmggr.exe c: -Enableと同じ処理を実行します。

EWF無効

このボタンで、DOSプロンプトのewfmggr.exe c: -Disableと同じ処理を実行します。

オーバーレイ情報

このボタンは、単にオーバーレイ情報を表示します。この情報は、DOSプロンプトのewfmggr.exe c: -Descriptionおよびewfmggr.exe c: -Gaugeを実行して提供された情報を組み合わせたものです。

ブートコマンドをクリア

このボタンで、DOSプロンプトのewfmggr.exe c: -NoCmdと同じ処理を実行します。

データ更新

このボタンで、DOSプロンプトのewfmggr.exe c: -Commitと同じ処理を実行します。

エンハンスド ライト フィルタ状態ツール

Windows XPeイメージには、EWF状態サービスが含まれます。このサービスによって、EWFの状態を示すアイコンがシステムトレイに表示されます。この状態表示アイコンは、EWFが無効な場合には赤色の鍵、有効な場合には緑色の鍵、次回の起動で設定が変更される状態の場合には黄色の鍵で表示されます。



EWFが破損した状態の場合は、Webで提供される標準の出荷イメージを使ってThin Client本体を再度フラッシュする必要があります。詳しくは、以下のWebサイトにあるホワイトペーパー『HP Compaq Thin Client Imaging Tool』（英語版）を参照してください。
http://h200006.www2.hp.com/bc/docs/support/UCR/SupportManual/TPM_339082-003_rev4_us/TPM_339082-003_rev4_us.pdf

Administratorとしてログオンしている場合は、アイコンを右クリックしてEWFの状態を選択することにより、EWFの状態を変更できます。



EWF Managerのコンソールユーティリティ（ewfmg.exe）とEWF状態サービスは個別のコードを実行するため、ewfmg.exeによる状態の変更はEWF状態アイコンに自動的に反映されません。

コマンドラインからEWFを変更した場合は、アイコンを右クリックして状態アイコンの表示を更新する必要があります（コンテキストメニューは、画面上の任意の場所でクリックすることにより閉じることができます）。[コントロール パネル]のEWFアプレットを使用して変更した場合は、状態アイコンの表示が自動的に更新されます。EWFアプレットは、常に最新の状態を反映します。

ローカル ドライブ

以下のセクションでは、Thin Clientのローカル ドライブについて説明します。

Z:ドライブ

Z:ドライブは、Thin Clientの論理ボード上にある揮発性メモリ（Ms-ramdrive）です。Z:ドライブは揮発性のドライブであるため、保持しておきたいデータの保存には使用しないことをおすすめします。RAMディスクの設定方法については、[12ページの「HP RAMディスク」](#)を参照してください。Z:ドライブを移動プロファイルに使用する方法については、このガイドの[34ページの「移動プロファイル」](#)を参照してください。

C:ドライブとフラッシュ

C:ドライブは、オンボードの不揮発性フラッシュ メモリ内にあります。C:ドライブには書き込まないことをおすすめします。C:ドライブに書き込むと、フラッシュの空き領域が減少します。



注意：フラッシュ メモリの空き領域が3 MB未満になると、Thin Clientの動作が不安定になります。

エンハンスド ライト フィルタが有効な場合、このフィルタはフラッシュ メモリの破損を防ぎ、キャッシュへの過度の書き込みが行われるとエラー メッセージを表示します。

通常の処理で書き込みフィルタ キャッシュに書き込まれる項目、また書き込みフィルタが無効な場合にフラッシュに直接書き込まれる項目には、お気に入り、作成された接続、および削除または変更された接続が含まれます。

ファイルの保存



注意：Thin Clientは、組み込まれたオペレーティング システムを一定量のフラッシュ メモリで使用します。保持しておきたいファイルは、Thin Clientではなくサーバ上に保存することをおすすめします。C:ドライブはフラッシュメモリ内にあるため、C:ドライブにデータを書き込むアプリケーションの設定には注意が必要です（特に、多くのアプリケーションはデフォルトでローカル システムのC:ドライブにキャッシュ ファイルを書き込むように設定されています）。ローカル ドライブに書き込む必要がある場合は、Z:ドライブを使用するようにアプリケーションの設定を変更してください。C:ドライブへの書き込みを最小限に抑えるには、「[ユーザ ログ アカウント](#)」の説明に従って設定する必要があります。

ネットワーク ドライブの割り当て

管理者およびユーザのどちらとしてログオンしていても、ネットワーク ドライブを割り当てることができます。Thin Clientの再起動後に割り当てを保持するには、以下の手順で操作します。

1. 現在のブートセッション中に書き込みフィルタ キャッシュを無効にするか、-commitコマンドを実行します。
2. **[ログオン時に再接続する]**チェック ボックスをオンにします。

ユーザとしてログオンしている場合は書き込みフィルタ キャッシュを無効することはできないため、ログオフしてから（シャットダウンまたは再起動はしないでください）管理者として再度ログオンし、書き込みフィルタを無効にすることにより、割り当てを保持することができます。

ユーザ管理ユーティリティを使用することによって、または管理者が認識している他の方法によって、リモートのホーム ディレクトリを割り当てることができます。

移動プロファイル

移動プロファイルは、C:ドライブに書き込むようにしてください。プロファイルのサイズは制限する必要があり、また、プロファイルはThin Clientの再起動後に保持されません。



移動プロファイルを機能させ、ダウンロードするためには、十分なフラッシュメモリ領域が必要です。場合によっては、ソフトウェア コンポーネントを削除して、移動プロファイルのために空き領域を確保する必要があります。

ユーザ ログ アカウント

ここでは、新しいユーザ アカウントとユーザ プロファイルの作成方法について説明します。

新しいユーザ アカウントの作成



注意: 新しいアカウントを作成したブートセッション中に、書き込みフィルタ キャッシュを無効にする必要があります。すべての永続的な変更がフラッシュに保存された後には、書き込みフィルタを有効にしておいてください。

ユーザ アカウントを作成するには、管理者としてログオンしている必要があります。アカウントの作成は、ローカルでもリモートでも行うことができます。ローカルのフラッシュ メモリおよびディスクの容量には制限があるため、追加するユーザの数は最小限に抑える必要があります。

新しいユーザ アカウントの作成には、ユーザ管理ユーティリティを使用します。ユーティリティを実行するには、[コントロール パネル]→[パフォーマンスとメンテナンス]→[管理ツール]の順にクリックします。

ユーザ プロファイル

新しいユーザ プロファイルは、レジストリ、ブラウザ プロファイル、およびICAとRDPの初期設定に格納されているユーザまたは管理者のデフォルトのアクセス設定を基にしたテンプレートから自動的に設定されます。ユーザまたは管理者のデフォルトのプロファイル設定が工場出荷時の設定から変更されると、変更された設定が新しいユーザ プロファイルに自動的に適用されます。

新しいユーザをデフォルト ユーザの特性に一致させるには、管理者はユーザをユーザ グループ内に作成し、新しいユーザを管理者グループにも追加する必要があります。デフォルトのユーザは両方のグループに属します。そのようにしないと、新しいユーザがローカル プリントを追加できません。ユーザが管理者グループに属していても、ユーザが行うことのできる操作には制限があります。

ユーザを作成するには、以下の手順で操作します。



注意：フラッシュ メモリのサイズに制限があるため、新しいユーザと既存のユーザが使用できるその他のアプリケーションで、ローカル ファイル システムに書き込みができないように設定することを強くおすすめします。同じ理由により、工場出荷時にインストールされているアプリケーションの設定を変更する場合も細心の注意を払ってください。

1. 管理者としてログインします。
2. **[管理ツール]**ウィンドウを開きます (**[スタート]**→**[コントロール パネル]**→**[パフォーマンスとメンテナンス]**→**[管理ツール]**の順に選択します)。
3. **[ユーザー マネージャ]**をダブルクリックして、**[ローカル ユーザーとグループ]**ウィンドウを表示します。
4. **[ユーザー]**フォルダをダブルクリックして、右側のパネルの内容を参照します。
5. メニュー バーの**[操作]**をクリックし、ドロップダウン メニューで**[新しいユーザー]**を選択します。**[新しいユーザー]**ダイアログ ボックスが表示されます。
6. ユーザ名とパスワードを入力し、属性を選択します。
7. **[作成]**をクリックし、**[閉じる]**コマンド ボタンをクリックします。
8. **[ローカル ユーザとグループ]**ウィンドウの左側のパネルで、**[ユーザー]**フォルダを選択 (強調表示) します。
9. 右側のパネルで、作成したユーザの名前をダブルクリックします。ユーザ プロパティのダイアログ ボックスが表示されます。
10. **[所属するグループ]**タブ ダイアログを開きます。
11. **[追加]**をクリックします。**[グループの選択]**ダイアログ ボックスが表示されます。

-
12. [選択するオブジェクト名を入力してください]フィールドに「Administrators」と入力します。[名前の確認]コマンド ボタンが有効になります。
 13. [名前の確認]をクリックし、[OK]をクリックします。
 14. これで、新しく作成されたユーザが管理者グループとユーザ グループの両方のメンバになり、デフォルト ユーザ アカウントの権限に一致します。

リモート管理とファームウェアのアップグレード

ここでは、お使いのThin Clientに適用できるリモート管理機能とファームウェアのアップグレード方法について説明します。

Altiris Deployment Solutionソフトウェア

Altiris Deployment Solutionソフトウェアは、完全な機能を備えたリモート管理ツールセットです。このソフトウェアは、Thin ClientにインストールされているAltiris リモート エージェントとPXEサーバユーティリティを通じて、Thin Clientにアクセスします。Altirisを使用することで、管理者が各Thin Clientサイトを直接操作することなく、ファームウェアのアップグレードを含めたThin Clientの管理を行うことができます。

Altirisの使用方法について詳しくは、Altirisのヘルプ ドキュメントを参照してください。

アドオン モジュール

アドオン モジュールのインストールが必要な場合、管理者はAltiris Deployment Solutionを使用してThin Clientを管理する必要があります。変更を保存するには、必要に応じて書き込みフィルタの無効/有効を切り替える必要があります。



注意：フラッシュ メモリの空き領域が3 MB未満になると、Thin Clientの動作が不安定になります。



アドオン モジュールを機能させ、ダウンロードするためには、十分なフラッシュ メモリ領域が必要です。場合によっては、ソフトウェア コンポーネントを削除して、アドオン モジュールのために空き領域を確保する必要があります。

ファームウェアのアップグレード

Intel Preboot Execution Environment (PXE) は、クライアントがサーバからブリーブ環境をダウンロードできるようにするためのTCP/IP、DHCP、およびTFTPの間の対話を定義するプロトコルです。PXEを使用すると、組み込まれたオペレーティング システムや、ローカルのフラッシュ モジュールにインストールされたオペレーティング システムの起動より先に、ネットワーク上のサーバからクライアントを起動することができます。ネットワーク管理者は、PXEを使用してThin Clientをリモートで起動し、さまざまな管理タスクを実行できます。たとえば、ネットワークを通じてサーバからオペレーティング システムやその他のソフトウェアをThin Clientにロードすることが可能です。PXEクライアントはThin Clientにインストールされており、PXEサーバ コンポーネントはAltiris Deployment Solutionの一部です。



Citrix ICA の自動更新は、Thin ClientにインストールされているICA クライアントに対しては機能しません。ICA クライアントの更新は、標準のファームウェア アップグレード処理によって実装されます。

HP Compaq Thin Clientイメージング ツール

HP Compaq Thin Clientイメージング ツールは、HP Compaq t5000 Thin Clientの工場出荷時イメージを含むSoftPakの一部です。このユーティリティを使用すると、工場出荷時のイメージをThin Clientに復元できます。

このユーティリティを使用すると、以下の3つの操作を行うことができます。

- USB CD-ROM ドライブを使用した展開のためのブート可能CDを作成するために、CD作成ソフトウェアで使用するISOイメージを生成する
- USB メモリなどのUSB フラッシュ デバイス上に、ブート可能なフラッシュ イメージを作成する
- カスタム展開シナリオやPXEイメージで使用するために、イメージをディレクトリに展開する

このユーティリティに関する詳しい情報と使用方法については、HPのWebサイト (<http://www.hp.com/products/thinclientsoftware>、英語サイト) を参照してください。